

Authentication & Trust

ideas and status

What's it about? Who's it for?

- Describes the trust model between clients and domains.
- Describes an application layer protocol to authenticate a registered user to an agent domain.
- Describes what to do if you want to use the transport's authentication services (like OAuth or TLS Client Certs.)
- Written for implementers.

Status

- Minor updates over the last year.
- Needs expanded trust model section.

Ideas

- MUST all implementers implement agent identifiers?
 - qualified "no."
 - the spec can't FORCE an agent domain to issue agent identifiers.
 - the draft "defines mechanism, not policy."
 - should we be more explicit about it in the spec?

Ideas

- MD5 is the suck.
 - People working in the Security Area will laugh at us.
 - We use the "one way" feature of MD5.
 - RFC4270 says something about this.
 - There is at least one major deployment of the legacy protocol on which VWRAP is based that is dependent on MD5

Transport Authentication

- The current draft takes a "minimalist" approach to transport based authentication.
 - If you want to use transport authentication or authorization, you send an agent_login message without an authenticator in the message.
 - Both sides are to interpret this as "we're using OAuth or TLS Client certs to assert authentication or authorization"
 - Do we need to say more?